UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/830,127 | 04/22/2004 | Paul A. Gassoway | 063170.6962 | 7446 |

5073 7590 10/28/2009

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

| EXAMINER | |
|---|---|
| TRAORE, FATOUMATA | |
| ART UNIT | PAPER NUMBER |
| 2436 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 10/28/2009 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/830,127 | GASSOWAY, PAUL A. | |
| | Examiner | Art Unit | |
| | FATOUMATA TRAORE | 2436 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *23 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-5,7-10,12-21,23-26,28-37,39-42 and 44-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-5,7-10,12-21,23-26,28-37,39-42 and 44-55* is/are allowed.

6)☒ Claim(s) *56-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/01/2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

**DETAILED ACTION**

1. This is in response to the amendment filed June 23, 2009. Claims 1, 17 , 33 and 56 have been amended. Claims 6, 11, 22, 27, 38 and 43 have been cancelled. Claims 1-5, 7-10, 12-21, 23-26, 28-37, 39-42 and 44-60 are pending and have been considered below.

***Response to Arguments***

2. The 101 rejection regarding claims 1-5, 7-10, 12-21, 23-26, 28-37, 39-42 and 44-60 has been withdrawn in light of the amendments to the claims.

3. Applicant argues, "Applicant respectfully contends that the proposed Berger-Sobel combination fails to disclose, teach, or suggest each and every one of these limitations. For instance, the Office Action relies on Berger as disclosing adding an entry for the file to a database of known good software if the quantitative information exceeds a predetermined value. Office Action, pg. 4. Applicant respectfully disagrees. Berger is directed toward a method of detecting potentially malicious action of a potentially unsafe application. Belier, Abstract. While server system 130 may be "updated to reflect that a potentially unsafe application is now a known safe application or a known unsafe application," there is no teaching, disclosure, or suggestion that this update is performed "if the quantitative information exceeds a predetermined value." The examiner respectfully disagrees and submits that Berger teaches when detecting a potential unsafe file(unknown file), the file is sent to sandbox for further analyzing and processing based on the result of the further processing in the sandbox server the local database are updated. The examiner notes that the further processing of the file is time consuming which could take a couple of second to a couple of minutes. The examiner also notes that a

predetermined time can be any amount of time , therefore the examiner submits that Berger teaches a step of adding an entry for the file to a database of known good software if the quantitative information exceeds a predetermined value(*see paragraphs [0011], 47, [0052], [0061, [0068], [0074*]).

4. Applicant also argues that" he cited portions of Sobel similarly fail to disclose, teach, or suggest determining a number of times the file has been opened or the number of times an executable in the file has been executed. For at least these reasons, Applicant respectfully contends that Sobel fails to disclose, teach, or suggest the quantitative information required by Claim 56. Therefore, Applicant respectfully requests reconsideration and allowance of Claim 56 Applicant respectfully contend that Sobel fails to disclose, teach, or suggest the quantitative information required by Claim 56. Therefore, Applicant respectfully requests reconsideration and allowance of Claim 56", the examiner submit the newly found references to Dutta et al (US 7, 539,664) discloses the quantitative information (column 9, lines 34-43).In addition Liang et al US 2004/0205419 teaches the quantitative information (see paragraphs [0016], [0035], [00048], [0051], [0052]).

***Claim Rejections - 35 USC § 101***

5. The 35 U.S.C. 101 rejections to claims 1-10, 12-169 49, 50, 52, 53 and 56-60 have been withdrawn in light of the amendment to the claims. A0pplicant amended claim 33 the recite the limitation of a tangible computer storage medium. The examiner notes that putting the world tangible in front of the storage medium does not overcome the 101, the examiner also notes that there is no antecedent basis for the term storage medium in the specification, therefore examiner

suggest the used of "program storage device". The 101 rejection to claims 33-37, 39-42, 44-48, 54 and 55 has been maintained.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 56-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berger (US 2004/0123117) in view of Dutta et al (US 7,539,664).

***Claim 56***: Berger discloses a method for computer security, comprising:

identifying a file(paragraph [0084]);

i. determining whether an entry for the file exists in database of unfamiliar software(*If the application characteristic doesn't match either a known safe application characteristic or a known unsafe application characteristic, a determination is made in operation 208 that the potentially unsafe application is an unknown application)(paragraph [0047]; Fig. 3, steps 314-320)*;

*ii.* adding an entry for the file to a database of known good software if the quantitative information exceeds a predetermined value*(if application is safe or unsafe operation 320, flow moves to an update local configuration operation 322. In update local configuration operation 322, the local configuration, e.g., application characteristics, on server system 130 is updated to reflect that the*

*potentially unsafe application is now a known safe application or a known unsafe application ) (paragraphs [0068], [0081]);* and

iii. allowing the opening of the file to continue if the database of known good software includes the entry for the file(*paragraph[0084*]).

Berge does not explicitly discloses determining quantitative information regarding the file, the quantitative information selected from the group consisting of a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed. However Dutta et al discloses a method for operating a rating server, which determining quantitative information regarding the file, the quantitative information selected from the group consisting of a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been *executed (the search result post-processor can monitor and record or log the number of times that a general file is opened or the number of times that an executable file has been executed. The search result post-processor could also monitor how long a file is kept before it is deleted (or moved) (column 9, lines 34-43).* Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Berger such as to use quantitative information. The motivation of doing so would have been to improve the performance of malicious computer code detection as taught by Dutta et al (column 1, lines 5-10).

***Claim 57***: Berger and Dutta et al disclose the method as in claim 56 above, and Burger further discloses a step of removing the entry for the file from the database of unfamiliar

software if the quantitative information exceeds a predetermined value(paragraph [0084]: Fig 2).

***Claim 58***: Berger and Dutta et al disclose the method as in claim 56 above, and Burger further discloses a step of preventing the opening of the file to continue if:

the database of known good software does not include the entry for the file(terminating)(paragraph [0049]); and

the file attempts a suspicious activity(deleting a file)(paragraph [0045]).

***Claim 59***: Berger and Dutta et al disclose the method as in claim 58 above, and Burger further discloses wherein a suspicious activity comprises updating a registry(paragraph [0033]).

***Claim 60***: Berger and Dutta et al disclose the method as in claim 58 above, and Burger further discloses wherein a suspicious activity comprises opening a second file(paragraph [0033]).

### *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes,

which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

Wednesday, October 14, 2009.

/F. T./

Examiner, Art Unit 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436